IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	)	Misc. No. 1:11-DM-3 No. 10-GJ-3793 No. 1:11-EC-3

MEMORANDUM OPINION

This matter comes before the Court on Petitioners' Objections to rulings issued by United States Magistrate Judge Theresa Carroll Buchanan regarding an Order issued after application under Title II of the Electronic Communications Privacy Act, known as the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.* In their Motion to Vacate (Doc. 1) and Motion to Unseal (Doc. 3), Petitioners moved to quash the Order, unseal the application seeking the Order, and publicly docket other related information. Magistrate Judge Buchanan denied the motion to vacate and granted in part and denied in part the motion to unseal, and Petitioners objected. For the reasons stated in this opinion, Petitioners' objections are DENIED.

I. BACKGROUND

As part of an ongoing criminal investigation, Respondent United States of America obtained a court order to turn over information pertaining to Petitioners, who were subscribers and users of certain websites and services of interest to the government. Petitioners Jacob Appelbaum, Rop Gonggrijp, and Birgitta Jonsdottir challenge the order and other rulings as Real Parties in Interest. Mr. Appelbaum is a resident and citizen of the United States and is a computer security expert. Doc. 3 at 10. Mr. Gonggrijp is a Dutch citizen and a computer security expert. Doc. 3 at 11. Birgitta Jonsdottir is a citizen and resident of Iceland, and currently serves as a member of the Parliament of Iceland. Doc. 3 at 10. Each Petitioner used the Internet to

communicate with the Twitter social networking service.[1]

A. Twitter

Petitioners are Twitter subscribers. Twitter is a social networking service that permits users[2] to post pithy messages using short communications called "tweets," and to read the tweets of other users.[3] Users can monitor, or "follow," other users' tweets, and can permit or forbid access to their own tweets. In addition to posting their own tweets, users may send messages to a single user ("direct messages") or repost other users' tweets ("retweet"). Each Twitter user has a unique username. Mr. Appelbaum, for example, used the moniker `ioerror`. Mr. Gonggrijp was known as `rop_g`, and Ms. Jonsdottir used the name `birgittaj`.

As counsel for Mr. Applebaum stated at the hearing on February 15, 2011, a person signing up for the Twitter service must click on a button below a text box indicating that "[b]y clicking the button, you agree to the terms below," where the "terms" referred to are displayed in the text box. *See* Doc. 41 at 17; Ex. 1 attached to Decl. of Karen Bringola ("Bringola Decl."), Doc. 45-1 at 5. Those terms are listed in a small text box. *See* Doc. 45-1 at 5. The terms indicate that users agree to the Twitter Privacy Policy ("Privacy Policy"). *See* Ex. 3, attached to Bringola Decl. at 22-23; *see also Twitter Privacy Policy*, http://twitter.com/privacy (last accessed Nov. 9, 2011). Neither party disputes that Twitter users click on a button indicating agreement to the terms, including the Privacy Policy, as a practical condition of creating an account. *See* Doc. 41

[1] Three briefs have been submitted by amici. *See* Mem. of The Inter-Parliamentary Union, Doc. 32-2 at 2-5; Mem. of Christopher Soghoian *et al.*, Doc. 47-1; Br. of Steven M. Bellovin, *et al.*, Doc. 49. The Court thanks all amici for their contributions to the Court's consideration of this matter. The submission by Steven M. Bellovin *et al.*, Doc. 49, in particular, provided excellent background information to assist the Court in consideration of the issues before it.

[2] The terms "user," "customer," and "subscriber" are technically distinct under the Stored Communications Act, but the distinction is immaterial on the facts of this case. The Court therefore uses them interchangeably.

[3] Tweets are limited to 140 text characters, though many Twitter users post links to sites containing more verbose content. *See* Ex. 4 attached to Sears Decl., Doc. 2-4 at 2-9.

at 16-17. At the hearing before Magistrate Judge Buchanan on the motion to vacate, the following discussion took place:

> MR. KEKER [arguing the Motion to Vacate on behalf of all parties in interest]: And in a hearing we believe we could show that not nobody, but most people, the vast majority of people have no idea that Twitter collects the information about their whereabouts and--
>
> THE COURT: Well, your clients seem like pretty knowledgeable people, and they did agree to Twitter's privacy policy, did they not?
>
> MR. KEKER: They-- I wouldn't accept that they agreed to Twitter privacy policy.
>
> THE COURT: They were informed of it at any rate--
>
> MR. KEKER: They went ahead with Twitter in the face-- I have had those things pop up on my screen every time I have gotten a new program. I think their-- I have--
>
> THE COURT: So, you don't read them?
>
> MR. KEKER: I have never read the whole thing. So, saying that they agreed to it, it was jammed down their throat. Yes, it appeared on their screen, there is no question about that.
>
> THE COURT: Well, it would be a condition of creating a Twitter account, would it not?
>
> MR. KEKER: Correct, that's true.
>
> THE COURT: Okay. And they agreed to that, correct?
>
> MR. KEKER: They created a Twitter account, that's certainly true.
>
> THE COURT: All right. Subject to that. Okay.
>
> MR. KEKER: And that is one factor, I totally agree, that would be as useful factor for the Government in this hearing where you tried to figure out what a reasonable expectation of privacy is. But I would argue that there would be ways to overcome that.

Doc. 41 at 16-17. The Privacy Policy informs users about information collected upon registration of an account, as well as additional information collected by Twitter in the course of its operation. Bringola Decl. at 22-23. Twitter collects many types of usage information, including physical location, IP address, browser type, the referring domain, pages visited, search terms, interactions with advertisements, clicks on links, cookies, and other types. *Id.* The Privacy Policy further states that Twitter may disclose information about an account if Twitter believes it reasonably necessary to comply with a law, regulation or legal request, or to address fraud, security, or technical issues, or protect a person's safety. Bringola Decl. at 23.

B. IP Addresses

A computer attached to the Internet uses a unique numerical address called an Internet Protocol address, or IP address, to identify itself to other computers. *Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Svcs.*, 545 U.S. 967, 987 n.1 (2005) ("IP addresses identify computers on the Internet, enabling data packets transmitted from other computers to reach them."); *United States v. Yu*, 411 Fed. Appx. 559, 560 n.1 (4th Cir. 2010) ("Each computer connected to the Internet is assigned a unique numerical address, otherwise known as an Internet protocol or IP address, to identify itself and facilitate the orderly flow of electronic traffic.") (quoting *Peterson v. Nat'l Telecomm'n & Info. Admin.*, 478 F.3d 626, 629 (4th Cir. 2007)). In computer terms, an IP address is a 32-bit integer that can be stamped on network communications or translated into human-readable format. The most basic communication standard underlying the Internet, called the Internet Protocol, uses IP addresses to transmit bundles of data, called "packets," through the network. Amicus Br. of Steven Bellovin, Ph.D., *et al.* ("Bellovin Br."), Doc. 49 at 5. Each IP address is a numeric address, usually expressed as four numbers separated by periods (such as a.b.c.d, where a, b, c, and d represent numbers from 0 to 255). Bellovin Br. at 5.

Special computers called "routers" communicate packets among themselves through a patchwork of interconnections and maintain a database that specifies how to direct each packet in the proper direction. *See* Bellovin Br. at 5-6. Each packet is stamped with a source IP address and a destination IP address, and every time a router receives a packet, it examines the destination address, looks up routing information for that address in the database, and forwards the packet toward the right network. Bellovin Br. at 5-6. This process is repeated until the packet reaches a router that can transmit directly to the destination IP address. Clearly, correct IP

addressing information is essential to Internet technology.[4]

A human user may not know the specific IP address assigned to his network connection, or the IP address of a remote computer or website, even though the computer must know those addresses as a prerequisite to Internet communications. Bellovin Br. at 6-7. Nowadays, most Internet users access a system called the Domain Name System, or DNS, that allows persons to use a computer name (such as twitter.com or www.vaed.uscourts.gov) as a substitute for an IP address. *Peterson*, 478 F.3d at 629. Thus, when a person attempts to access a named computer, the person's computer finds the IP address of the remote site by matching, or "resolving," the name to the proper IP address, then contacts the website over the Internet using that IP address.[5]

From the perspective of the destination computer, it is an extraordinarily simple task to determine the IP address of the computer seeking to access it. Bellovin Br. at 7; *see also United States v. Christie*, 624 F.3d558, 563 (3d Cir. 2010) ("IP addresses are also conveyed to websites that an internet user visits, and administrators of websites . . . can see the IP addresses of visitors to their sites."). Most websites maintain standard logs of connecting IP addresses, along with date and time information, and may even include information about the user associated with the connection. Bellovin Br. at 7. Such information is routinely gathered to evaluate usage patterns, engage in site marketing analysis, troubleshoot problems, or to gather feedback. Some commercial enterprises even collect IP address information to provide location data associated with particular users, presumably for marketing purposes. Bellovin Br. at 8; *see* Bringola Decl. at

---

[4] Some technologies use the Internet Protocol to transmit media content to consumers, though they do not send information over the actual Internet. *See WPIX, Inc. v. ivi, Inc.*, 765 F. Supp. 2d 594, 612 n.24 (S.D.N.Y. 2011) ("Using Internet Protocol to deliver video programming (commonly referred to as IPTV) is distinct from using the Internet. . . . IPTV video is typically delivered through a closed, end-to-end system in which the distributor controls the wires and routers right up until the subscriber's home." (citations and quotations omitted)).

[5] The DNS resolution process emerged as the Internet's size and scope made everyday use of IP address information inefficient and awkward. *See Peterson*, 478 F.3d at 629.

22-23.

Each network attached to the Internet, whether privately or publicly owned, is associated with a particular block of IP addresses. Bellovin Br. at 5-6. Some of these networks assign a unique IP address to each attached device, whereas others assign an IP address to a device that allows a private network to share a single IP address. Bellovin Br. at 6. Some networks assign one predefined address to each attached device ("static" addressing), whereas others assign addresses from a pool of available addresses ("dynamic" addressing). *See* Bellovin Br. at 6; *see also Christie*, 624 F.3d at 563 ("Residential internet customers typically connect to the internet through an internet service provider ('ISP'). Each time a customer connects, the ISP assigns a unique identifier, known as an IP address, to the customer's computer terminal. Depending on the ISP, a customer's IP address can change each time he logs on to the internet."). If a portable device (like a laptop) moves from one network to another, such as between a home office and a coffee shop, the IP address of the device changes. Bellovin Br. at 4.

IP address information, by itself, cannot identify a particular person. As amici point out, IP address information can identify a particular personal computer, subject to the possibility of dynamic addressing noted above, but it can also identify a device that connects to another network, such as an internal home or office network. Bellovin Br. at 4. Moreover, though IP addresses can assist in identification, they have been found inadequate to identify a particular defendant for the purposes of service of process. *See, e.g.*, *Call of the Wild Movie, LLC v. Does 1-1,062*, 770 F. Supp. 2d 332, 346-48 (D.D.C. 2011) (denying motions to quash subpoenas issued for jurisdictional discovery of unnamed defendants using known IP addresses); *Diabolic Video Prod., Inc. v. Does 1-2099*, No. 10-cv-5865, 2011 WL 3100404, at *2 (N.D. Cal. May 31, 2011) (for proper service of process, IP addresses must be tied to a name and address in physical

space). Even if certain actions are traceable to an IP address, therefore, attributing those actions to a real person requires evidence associating a real world person with the residuum of his more transient and diaphanous presence in cyberspace.

C. The Twitter Order

On December 14, 2010, upon *ex parte* application by the government, Magistrate Judge Buchanan issued an order ("Twitter Order") under 18 U.S.C. § 2703(d) instructing Twitter, Inc. to produce specified electronic records to the government. Ex. 1 attached to Doc. 2-1, Decl. of Stuart A. Sears ("Sears Decl."), at 2-4. Magistrate Judge Buchanan found that Respondent had "offered specific and articulable facts showing that there [were] reasonable grounds to believe that the records or other information sought [were] relevant and material to an ongoing criminal investigation," that "the information sought [was] relevant and material to an ongoing criminal investigation, and that prior notice of [the Twitter Order] to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation[.]" Sears Decl. at 2. She therefore ordered that the application and Twitter Order be sealed, and ordered Twitter not to disclose the existence of either the Twitter Order or the investigation until authorized by the Court. Sears Decl. at 3.

The Twitter Order required Twitter to produce specified electronic records related to Petitioners and their usernames, as well as records concerning Wikileaks, Julian Assange, and Bradley Manning. In particular, Respondent sought the following records:

> A. The following customer or subscriber account information for each account registered to or associated with Wikileaks; rop_g; ioerror; birgittaj; Julian Assange; Bradley Manning; Rop Gongrijp [*sic*]; Birgitta Jonsdottir for the time period November 1, 2009 to present:
>
> 1. subscriber names, user names, screen names, or other identities;
> 2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
> 3. connection records, or records of session times and durations;

4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
3. correspondence and notes of records related to the account(s).

Doc. 2-1 at 4.

On January 5, 2011, upon motion by Twitter and consent by the government, Magistrate Judge Buchanan unsealed the Twitter Order, finding that it was in the best interest of the investigation and authorizing Twitter to disclose the Twitter Order to its subscribers. Sears Decl., Ex. 2, Doc. 2-2 at 2.

D. Motion to Vacate and Motion to Unseal

On January 26, 2011, Petitioners filed a Motion to Vacate the Twitter Order and a Motion to Unseal certain court records. Docs. 1 & 3. The Motion to Vacate asked the Court to vacate the Twitter Order on various statutory and constitutional grounds. Doc. 1. The Motion to Unseal requested unsealing of a wide variety of materials, namely: "(1) all orders and documents filed in this matter before the Court's issuance of the December 14, 2010 Order requiring Twitter to provide information concerning Movants[]; (2) all orders and documents filed in this matter after issuance of the Twitter Order; (3) all similar judicial orders requiring entities other than Twitter to provide information concerning Movants' electronic communications and publications;[] and (4) all documents filed in connection with such other orders or requests for such orders[.]" Doc.

3 at 8. In addition, the Motion to Unseal requested public docketing of all orders issued under 18 U.S.C. § 2703. Doc. 3 at 16-17.

After extensive briefing, Magistrate Judge Buchanan issued an order and accompanying memorandum opinion on March 11, 2011 ("March 11 Order") in which she denied the Motion to Vacate, granted in part the Motion to Unseal, and kept under advisement the issue of public docketing. Docs. 38 & 39. On June 1, 2011, Magistrate Judge Buchanan issued an order ("June 1 Order") and accompanying memorandum opinion denying the request for public docketing. Docs. 60 & 61. Petitioners filed Objections to both Orders,[6] and their Objections are now before the Court. Docs. 45 & 64.

II. ANALYSIS

A. Standard of Review

Because this matter arises on objection to a magistrate judge's orders, the Court must determine the appropriate standard of review.[7] As a threshold matter, the Court must first address the basis for Magistrate Judge Buchanan's jurisdiction over this matter. Section 636(b) of U.S. Code, Title 28 grants jurisdiction as follows (in relevant part):

> (1) Notwithstanding any provision of law to the contrary--
>
> > (A) a judge may designate a magistrate judge to hear and determine any pretrial matter pending before the court, except a motion for injunctive relief, for judgment on the pleadings, for summary judgment, to dismiss or quash an indictment or information made by the defendant, to

[6] On May 19, 2011, Petitioners filed an Objection challenging what they referred to as Magistrate Judge Buchanan's "constructive denial" of their motion for public docketing. Doc. 58 at 15. After issuance of the June 1 Order, which explicitly denied their motion for public docketing, Petitioners filed another Objection. The Court finds that the Objection to constructive denial was superseded by the Objection to actual denial and is therefore moot.

[7] Though the correct standard of review is the deferential one, as explained *infra*, the Court has also conducted a *de novo* review and finds that Magistrate Judge Buchanan's findings and orders survive the more demanding scrutiny.

> suppress evidence in a criminal case, to dismiss or to permit maintenance of a class action, to dismiss for failure to state a claim upon which relief can be granted, and to involuntarily dismiss an action. A judge of the court may reconsider any pretrial matter under this subparagraph (A) where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law.
>
> (B) a judge may also designate a magistrate judge to conduct hearings, including evidentiary hearings, and to submit to a judge of the court proposed findings of fact and recommendations for the disposition, by a judge of the court, of any motion excepted in subparagraph (A), of applications for posttrial relief made by individuals convicted of criminal offenses and of prisoner petitions challenging conditions of confinement.
>
> (C) the magistrate judge shall file his proposed findings and recommendations under subparagraph (B) with the court and a copy shall forthwith be mailed to all parties.
>
> Within fourteen days after being served with a copy, any party may serve and file written objections to such proposed findings and recommendations as provided by rules of court. A judge of the court shall make a de novo determination of those portions of the report or specified proposed findings or recommendations to which objection is made. A judge of the court may accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge. The judge may also receive further evidence or recommit the matter to the magistrate judge with instructions.
>
> * * * *
>
> (3) A magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States.

28 U.S.C. § 636(b)(1), (3). The Federal Rules of Criminal and Civil Procedure implement § 636 in criminal and civil cases. *See* Fed. R. Crim. P. 59; Fed. R. Civ. P. 72.

Paragraph (1) of § 636(b) establishes the general contours of magistrate judge referral jurisdiction. A district judge may refer certain pretrial matters to the magistrate judge, and the

magistrate judge's orders issued under this authority may be reversed if "clearly erroneous or contrary to law." 28 U.S.C. § 636(b)(1)(A). Alternatively, a district judge may designate a matter for hearing and issuance of a report and recommendation by a magistrate judge. 28 U.S.C. § 636(b)(1)(B). Upon timely objection, the district court performs a *de novo* review of the report and recommendation before disposing of the matter. 28 U.S.C. § 636(b)(1)(C). If a matter is not covered by the provisions of paragraphs (1), the catch-all provision in paragraph (3) allows the district courts to "experiment in the assignment of other duties to magistrates which may not necessarily be included in the broad category of 'pretrial matters.'" H. Rep. No. 94-1609, at 10 (1976), *reprinted in* 1976 U.S.C.C.A.N. 6162, 6172; *see also* S. Rep. No. 94-625 (1976). Neither the federal criminal nor civil rules implement paragraph (3).

Petitioners contend that the Objections are offered under either Federal Rule of Criminal Procedure 59(b) or Federal Rule of Civil Procedure 72(b), both which follow § 636(b)(1)(B) in requiring *de novo* review of all dispositive orders issued by magistrate judges. Doc. 45 at 12; Doc. 64 at 11-12. Because denial of both Motions addressed all the relief requested, Petitioners argue, the denial was dispositive and the Court should review both orders under the *de novo* standard set forth in § 636(b)(1)(B).

The government counters that Rule 59(b) is inapplicable because it applies only where a magistrate has issued "proposed findings and recommendations." Fed. R. Crim. P. 59(b). Because no such findings or recommendations were issued here, the government argues, Rule 59(b) cannot apply. Moreover, the government argues, these Objections arise under Rule 59(a) of the Federal Rules of Criminal Procedure, which applies § 636(b)(1)(A) to criminal proceedings because they relate to a § 2703 order issued as part of a criminal investigation. The magistrate judge's orders "[do] not dispose of a charge or defense" under Fed. R. Crim. P. 59(a), that is, a

substantive crime or defense, but ordered the disclosure of records by a third party in the course of an ongoing investigation. Therefore the Motions below are non-dispositive pretrial orders under Federal Rule of Criminal Procedure 59(a) and 28 U.S.C. § 636(b)(1)(A). Doc. 55 at 2-5.

By its terms, § 636(b)(1)(A) cannot control because, as far as the Court knows, no event has occurred that would trigger Petitioners' right to trial by jury, and thereby render this a typical "pretrial matter." Nor does § 636(b)(1)(B) control, because no judge referred this matter to Magistrate Judge Buchanan for issuance of a report and recommendation, either by order or standing order. Instead, this matter fits within the catch-all provision of § 636(b)(3), which permits assignment of "such additional duties as are not inconsistent with the Constitution and laws of the United States." 28 U.S.C. § 636(b)(3). Neither party has hinted that determination of the matter at hand is inconsistent with either the Constitution or federal law, and this Court is unaware of any basis for such a conclusion. The Court therefore concludes that magistrate judge jurisdiction was proper under § 636(b)(3). Accordingly, no rule of procedure governs the standard of review here. Because this grant of jurisdiction is "not restricted in any way by any other specific grant of authority to magistrates," H. Rep. No. 95-1609, at 10 (1976), *reprinted in* 1976 U.S.C.C.A.N. 6162, 6172, the Court next considers what standard of review should apply.

Urging *de novo* review, Petitioners rely on *Aluminum Co. of America v. EPA* (*ALCOA*), where the Fourth Circuit held that a motion to quash an administrative warrant was a dispositive motion under either § 636(b)(1) or § 636(b)(3) because the motion to quash contained all the requested relief. 663 F.2d 499, 501-02 (4th Cir. 1981). They argue that Magistrate Judge Buchanan's denial of Petitioners' motions to vacate and to unseal addressed all the relief requested in this matter, and no other requests remained outstanding. Therefore, they argue, the motion to vacate and the motion for unsealing constitute one demand for relief and are subject to

the same standard of review. The government distinguishes *ALCOA* as pertaining only to an administrative investigation proceeding, not a grand jury proceeding. Moreover, the government argues, the Orders entered by the magistrate judge here did not dispose of the underlying grand jury investigation, and therefore could not be dispositive.

Though *ALCOA* applied *de novo* review where denial of a single motion for relief—in that case a motion to quash—resulted in the disposition of the entire action, the situation here is not analogous. No proceeding, whether a grand jury or other investigation, was terminated by Magistrate Judge Buchanan's orders. Petitioners filed the two motions here on January 26, 2011, then filed another motion for unsealing on January 31, 2011. Docs. 1, 3, & 17. On September 20 and October 11, 2011, Petitioners filed additional sealed motions for further relief. Docs. 75, 78, 80, & 82. Disposition of any one of these orders would not terminate the rest of the orders. No preclusive consequences arise from denial of Petitioners' motions. No rule prevents other parties from filing motions in this case. Indeed, Twitter, Inc. filed a motion on February 8, 2011, and amici filed motions on February 14, March 29, and March 31, 2011. In short, this matter is ongoing, and resolution of Petitioners' objections does not constitute "dispositive" relief under § 636.

Moreover, an administrative agency conducted the investigation in *ALCOA*, and there was no hint that the judicial branch could either terminate or supervise the agency's investigation. Here, by contrast, the underlying investigation apparently involves a grand jury, which despite its independent status, is supervised by the judicial branch. *United States v. Williams*, 504 U.S. 36, 47-48 (1992) ("The grand jury requires no authorization from its constituting court to initiate an investigation, nor does the prosecutor require leave of court to seek a grand jury indictment. And in its day-to-day functioning, the grand jury generally operates

without the interference of a presiding judge." (citations omitted)); *United States v. U.S. Dist. Ct. for S. Dist. Of W. Va.*, 238 F.2d 713, 722 (4th Cir. 1957) ("While the grand jury is summoned, empaneled and sworn by the court, it is essentially independent of court control."). A grand jury terminates its operations when discharged by the court. *See* Fed. R. Crim. P. 6(g); *see generally U.S. Dist. Ct. for S. Dist. Of W. Va.*, 238 F.2d at 722.

For these reasons, administrative subpoenas are "treated differently than other subpoenas in that they are final, appealable orders," a fact which weighs in favor of a conclusion that quashing only of administrative subpoenas should be treated as dispositive under § 636. *In re Oral Testimony of a Witness Subpoenaed Pursuant to Civil Investigative Demand No. 98-19*, 182 F.R.D. 196, 201-02 (E.D. Va. 1998). Specifically, "district court orders enforcing subpoenas in connection with grand jury proceedings or criminal or civil trials are not immediately appealable, absent a contempt citation, because such appeals would greatly delay the judicial process; orders enforcing subpoenas in connection with administrative investigations, by contrast, may be appealed immediately because there is no judicial proceeding in process that such appeals would delay." *Reich v. Nat'l Eng'g & Contracting Co.*, 13 F.3d 93, 95-96 (4th Cir. 1993). The problems of delay are the same for § 2703 orders as they are for search warrants, grand jury subpoenas, and other types of subpoenas. The Court thus concludes that *Reich*'s reasoning is appropriate here, and Petitioners' motions are not dispositive within the meaning of 28 U.S.C. § 636. Because the motions are not dispositive, the Court reviews their denial under a more deferential standard.

The Court finds that the appropriate standard of review is that specified in § 636(b)(1)(A), that is, whether the magistrate judge's order is "clearly erroneous or contrary to law." 28 U.S.C. § 636(b)(1)(A). Three factors weigh in favor of applying the standard of review

set forth in (b)(1)(A). First, as the Fourth Circuit and other courts have noted, the standard of review question raises practical concerns that weigh in favor of the (b)(1)(A) standard. Requiring *de novo* review as a general matter would render the investigation open to significant interference and delay. Petitioners could file seriatim motions for relief, each requiring *de novo* review by a district judge. This would transform what has historically been a series of *ex parte* proceedings constrained by judicial review into an adversarial contest of attrition. Interested parties would have the power to effectively halt or direct the course of the investigation, or to impose a significant procedural burden on it. The grand jury may not be used as "a pawn in a technical game," and the Constitution and federal law require no such result. *See U.S. Dist. Ct. for S. Dist. Of W. Virginia*, 238 F.2d at 72 (quoting *United States v. Johnson*, 319 U.S. 503, 512 (1943) (Frankfurter, J.)).

Second, the motions at issue here are the functional equivalent of the "pretrial matters" referred to in § 636(b)(1)(A), and the magistrate judge's decisions on them are therefore entitled to the same deference. The magistrate judge is in the best position to understand how her rulings will affect the government's investigation, and discretion is therefore most appropriately vested with her. The pretrial matters specifically exempted from the deferential standard under (b)(1)(A) are dispositive or have some effect on the substantive claims of a particular case, permitting a division of labor in which the magistrate handles procedural issues while allowing the district judge to focus on the merits of the case. The district judge therefore appropriately defers to the judgment of the magistrate judge in such matters.

Third, Fourth Circuit case law indicates that the Court should review the denial of Petitioners' motions to unseal under the deferential standard. The Court's decision here is constrained by *Media Gen. Operations, Inc. v. Buchanan* (*Media General*), 417 F.3d 424, 429

(4th Cir. 2005) (citing *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 65 (4th Cir. 1989)). Though *Media General* did not involve the standard of review for a district judge reviewing a magistrate judge's sealing decisions regarding § 2703 orders, it did speak of vesting discretion to seal or unseal in the judicial officer who issued a search warrant. "The decision to seal or grant access to warrant papers is committed to the sound discretion of the judicial officer who issued the warrant and reviewed for abuse of discretion." *Media General*, 417 F.3d at 429 (quotations omitted). Applications for § 2703 orders are just as sensitive as warrant papers, and the Court can find no material distinction between the two processes with respect to unsealing. The Court therefore holds that denial of Petitioners' various motions to unseal should be reviewed deferentially to determine if the denials constitute an abuse of discretion.

Petitioners cite several other inapposite cases in support of their bid for *de novo* review. The case of *Virginia Dep't of State Police v. Washington Post*, 386 F.3d 567, 575 (4th Cir. 2004) is irrelevant to the standard of review issue presented here. The language cited by Petitioners refers to the standard of review on appeal to the Fourth Circuit, not district judge review of a magistrate judge's decision. They also cite *In re Application & Affidavit for a Search Warrant*, 923 F.2d 324, 326 n.2 (4th Cir. 1991) for the proposition that the decision to grant or deny access is generally best left to the "trial court," which Petitioners argue is a district judge, not a magistrate judge. Doc. 64 at 11-12. *In re Application & Affidavit* is not relevant here, however, because that case addressed whether voir dire could be properly referred to a magistrate judge. It specifically noted that a district judge has superior familiarity with "the intricate workings of criminal trial procedures, the varying methods of voir dire, jurors' responses to pretrial publicity, and whether a defendant can be granted a fair trial." *In re Application & Affidavit*, 923 F.2d at 327-28. Here, by contrast, the situation is reversed: magistrate judges handle most orders related

to grand jury proceedings, which are (to borrow the Fourth Circuit's language) grist for the magistrate judges' mill, so district judges rightly defer to magistrate judges' discretion. Moreover, Petitioners have not provided a persuasive reason for the Court to ignore the Fourth Circuit's standard from *Media General*, which makes clear that a decision to grant access is committed "to the sound discretion of the judicial officer who issued the warrant and [is] reviewed for abuse of discretion." 417 F.3d at 429 (quotations omitted).

B. Issuance of the Twitter Order

Petitioners challenge Magistrate Judge Buchanan's ruling that they do not have standing to challenge the Twitter Order, that issuance of the Twitter Order was proper under the Stored Communications Act, and that issuance of the Twitter Order did not violate the Fourth Amendment.[8] Petitioners also object that issuance of the Twitter Order violated their rights under the Due Process Clause and the First Amendment, and that regardless of whether any particular constitutional violation has occurred, constitutional avoidance justifies discretionary action to vacate the Twitter Order.

1. Stored Communications Act

Congress enacted the SCA as Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (1986) (*codified as amended at* 18 U.S.C. §§ 2701–2711 (2010)), which was intended to extend enhanced privacy protections to then-nascent forms of telecommunications and computer technology like cellular phones, pagers, and electronic mail. *See* S. Rep. No. 99-541 at 4 (1986), *reprinted at* 1986 U.S.C.C.A.N. 3555, 3559; *see*

[8] Petitioners admit that the SCA limits the remedies available to "non-constitutional" violations, but appear to argue that the statute be construed to find a statutory right to oppose the Twitter Order. Doc. 45 at 13-14. The Court therefore construes Petitioners' argument as a claim that the SCA confers standing upon them to challenge the Twitter Order.

generally Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-13 (2008). The core of the SCA is 18 U.S.C. § 2703, which establishes procedures by which the government may obtain access to electronic communications and information.

Section 2703 distinguishes between "contents" and non-content "records." 18 U.S.C. § 2703; *see Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). If the government seeks *content* information about a communication, that is, "information concerning the substance, purport, or meaning of that communication," paragraphs (a) and (b) apply. 18 U.S.C. §§ 2510(8), 2703(a)-(b), 2711. If the government seeks non-content *records*, as it does here, paragraph (c) controls, and provides different procedural protections. 18 U.S.C. § 2703(c). The Twitter Order was issued under paragraph (c), which enumerates particular records subject to disclosure, including the subscriber or customer's name, address, telephone connection records or records of session times and durations, length and type of service used, telephone number or temporarily assigned network address, and method of payment. *Id.* The government need not notify the customer or subscriber of a records request under paragraph (c). 18 U.S.C. § 2703(c)(3).

If the requirements are satisfied, a court order "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The SCA authorizes limited challenges to orders issued under § 2703. A service provider from whom disclosure is ordered may make a prompt motion to "quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." *Id.* A subscriber or customer,

by contrast, may bring a statutory challenge to a § 2703 order issued pursuant to 18 U.S.C. § 2704 or in a post-execution remedy set forth elsewhere in the chapter. Under § 2704, the subscriber or customer may only challenge an order containing a requirement that the service provider create a backup copy of certain communication contents. 18 U.S.C. § 2704(b)(1)(A). If the order contains such a provision, the service provider must maintain the backup copies for a period of time. *See* 18 U.S.C. § 2704(a)(3).[9]

(I) Statutory Standing

Magistrate Judge Buchanan concluded that § 2704 does not apply here because the Twitter Order sought non-content records, and no other provision of the SCA authorizes a pre-execution challenge. Therefore, she held, the SCA forbids the subject of a § 2703 order from challenging the order.[10] Petitioners challenge that conclusion. The parties do not dispute that the Twitter Order sought non-content records, nor do they dispute that § 2704 is inapplicable here. Rather, they dispute the significance of § 2704 within the statutory scheme. Petitioners argue that Magistrate Judge Buchanan's statutory analysis is incorrect, but can point to no provision of the SCA explicitly authorizing a pre-execution motion to vacate like the one here. The government argues that because § 2704 is the only provision of the SCA permitting a subject to contest a § 2703 order, and § 2704 does not apply here, Petitioners have no statutory standing to challenge the Twitter Order on non-constitutional grounds.

Viewed within the SCA as a whole, it is clear that the heightened procedural

[9] An exception to the challenge provision attempts to mitigate the risk of data destruction or tampering. 18 U.S.C. § 2704(a)(5).

[10] This issue was briefed differently before Magistrate Judge Buchanan, and neither side adopts Magistrate Judge Buchanan's analysis on this point. The Court therefore sets forth its own analysis.

requirements applicable to § 2704 backup orders are the exception, not the rule.[11] A customer whose backup copy is to be provided to the government receives special notice and opportunity to object, and a service provider may not provide the backup copy to the government until the challenge has been settled. 18 U.S.C. § 2704(a)(2), (4). The SCA creates no analogous process for other orders. Because Congress clearly provided pre-disclosure protections for one type of § 2703 order but not for others, the Court must infer that Congress deliberately declined to permit challenges for the omitted orders.[12] Had Congress intended to permit pre-execution challenges, Congress could easily have done so, whether in § 2703 or elsewhere. It did not. The total omission of any additional pre-execution opportunity for a subscriber or customer to challenge a § 2703 order reflects Congress's intention to prevent such challenges. *See NISH v. Cohen*, 247 F.3d 197, 203-04 (4th Cir. 2001) ("The omission by Congress of language in one section of a statute that is included in another section of the same statute generally reflects Congress's intentional and purposeful exclusion in the former section."); *Piney Mountain Coal Co. v. Mays*, 176 F.3d 753, 765 (4th Cir. 1999); *see also Russello v. United States*, 464 U.S. 16, 23 (1983) ("Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion. Had Congress intended to restrict § 1963(a)(1) to an interest in an enterprise, it presumably would have done so expressly as it did in the immediately following subsection (a)(2)." (punctuation and citations omitted)); *Ayes v. U.S. Dep't of Veterans Affairs*, 473 F.3d 104, 110-11 (4th Cir. 2006) (citing *Barnhart v. Peabody Coal Co.*, 537 U.S.

[11] As Magistrate Judge Buchanan observed in the March 11 opinion, the SCA provides greater protection for "contents" of electronic communications than it does for "records" of those communications. In doing so, the SCA incorporates the distinction between content and non-content information set forth by the Supreme Court in *Smith*. 442 U.S. at 741-42. Section 2704 applies only to § 2703 orders seeking "contents."

[12] Indeed, Congress only mandated a heightened notice requirement for disclosure of the backup copies to the government, not at creation by the service provider.

149, 168 (2003)).

Even where Congress provides remedies to subjects of § 2703 orders, they exist as carefully crafted post-execution, not pre-execution, remedies. The SCA forbids a victim of an unlawful order from seeking legal redress from a service provider who discloses information in accordance with the terms of a § 2703 order, but permits a damages award to any person aggrieved by an intentional or knowing violation of the SCA. 18 U.S.C. §§ 2703(e), 2707(a). The SCA specifically exempts the government from liability for damages, but provides that a government violation of the SCA or the Constitution will trigger potential disciplinary proceedings. 18 U.S.C. § 2707(a)-(d). The SCA makes clear that the statutory remedies are the only remedies: "The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Based on this evidence, the Court concludes that the Stored Communications Act does not confer upon Petitioners a right to seek non-constitutional review of the Twitter Order. The Court declines to imply a statutory right to notice or a pre-execution hearing. The magistrate judge correctly concluded that Petitioners have no statutory standing to bring the Motion to Vacate the Twitter Order on non-constitutional grounds.

(II) Sufficiency of the evidence

Even if Petitioners have standing to object to the Twitter Order on non-constitutional grounds, Petitioners fail to show that Magistrate Judge Buchanan incorrectly issued the Twitter Order under § 2703(d). Petitioners allege that the Twitter Order was mistakenly issued because the government did not offer "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Before analyzing whether the § 2703 standard was satisfied, however, it is important to note that although the Twitter Order itself has been unsealed, the confidential factual affidavit submitted in support of the § 2703(d) application remains under seal. The Court has thoroughly reviewed the application in consideration of this matter.

Petitioners argue that because most of their Twitter activity was unrelated to Wikileaks, the application could not have met the § 2703(d) standard. Doc. 45 at 15. The Court disagrees. The sealed affidavit clearly sets forth specific and articulable facts showing reasonable grounds to believe that the information sought by the government was relevant and material to the investigation. The government's factual basis for the Twitter Order was significantly more concrete than the "mere speculation" or "blind request" that Petitioners complain of. Doc. 45 at 15-16. Moreover, the information sought was clearly material to establishing key facts related to an ongoing investigation, and would have assisted a grand jury in conducting an inquiry into the particular matters under investigation.

Petitioners further object that the Twitter Order was unlawful because "the government cannot be permitted to blindly request everything that 'might' be useful and ignore § 2703's materiality requirement." Doc. 45 at 16; Doc. 30 at 9-10. In other words, Petitioners object to the Twitter Order as overbroad because it seeks records, only some of which are material. The Twitter Order is not overbroad. First, as the Court will explain, it is clear that no constitutional right is implicated by disclosure of the sought records, so there is no need for constitutional avoidance or narrow tailoring. Second, § 2703(d) requires the government to show only "reasonable grounds to believe that the . . . records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The government need not show actual relevance, such as would be required at trial. The government has shown ample

grounds for its request under this standard. Third, all evidence exists in a factual context, and to understand evidence one must understand its context. Some amount of what Petitioners consider "overbreadth" is always necessary to establish context for facts that are indisputably relevant and material. The probability that some gathered information will not be material is not a substantial objection at this stage.

Fourth, the notion that the government must determine the scope of a § 2703 order with great precision before the order can be issued is quite incorrect. The purpose of a criminal investigation is to find out whether crimes have occurred; to find out whether crimes have occurred, the government must conduct a factual investigation. To restrict the government's inquiry to a single, narrow theory before it can rule out other theories would impose a significant and unjustified burden on law enforcement. The Court holds that Magistrate Judge Buchanan did not abuse her discretion, and correctly applied the § 2703(d) standard.

2. Fourth Amendment

Petitioners also challenge issuance of the Twitter Order under the Fourth Amendment. In the March 11 Order, Magistrate Judge Buchanan rejected Petitioners' claim that they had a reasonable expectation of privacy in Internet Protocol (IP) address information sought by the Twitter Order and that warrantless disclosure of that information violated the Fourth Amendment. Specifically, she rejected Petitioners' argument that the IP address information sought by the Twitter Order was inappropriately revealing about the interior of Petitioners' homes and therefore protected by the Fourth Amendment. She determined that Petitioners' Fourth Amendment argument falls under the sword of the third-party doctrine, which states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44 (telephone numbers); *see United States v. Miller*, 425

U.S. 435, 442 (1976) (bank records). Petitioners object to both conclusions.

(I) Reasonable Expectation of Privacy in IP Address Information

As a general rule, the Fourth Amendment forbids warrantless searches. *City of Ontario, California v. Quon*, --- U.S. ---, 130 S. Ct. 2619, 2630 (2010), (citing *Katz v. United States*, 389 U.S. 347, 357 (1967)). To determine if the Twitter Order effected a search, therefore, the Court must ask whether Petitioners had a reasonable expectation of privacy in IP address information, as collected and stored by Twitter.[13] *See Katz*, 389 U.S. at 353; *see also id.* at 360 (Harlan, J., concurring). Petitioners argue that they have a reasonable expectation of privacy in IP address information because it reveals information about private spaces, and because the information was not voluntarily conveyed in the course of Petitioners' use of Twitter. Doc. 45 at 20-24. The government responds that Petitioners have no Fourth Amendment interest in IP address information because the mere possibility that IP address records could be used to discern a physical location does not create a protected Fourth Amendment interest. Doc. 55 at 15-22. Moreover, the government argues, Petitioners voluntarily conveyed their IP address information to Twitter, relinquishing any reasonable expectation of privacy in that information under the third-party doctrine.

The Court should note at the outset that neither the Supreme Court nor this Circuit has clearly addressed the treatment of IP addresses under the Fourth Amendment. The Fourth Circuit has, however, addressed government attempts to obtain subscriber information, including IP address information, *United States v. Hambrick*, 225 F.3d 656 (tbl.), 2000 WL 1062039, at *1-*2 (4th Cir. 2000) (defective subpoena requested IP address information), or information that would

[13] The Twitter Order did not seek IP address information obtained through government interception of communications between Petitioners and Twitter. That would pose a dramatically different scenario than presented here. Rather, the Twitter Order sought records—kept by Twitter in the course of its operations—about Petitioners' interactions with their Internet service.

help correlate a particular IP address with a particular user. *United States v. Bynum*, 604 F.3d 161, 164 n.2 (4th Cir. 2010) (approving collection of non-IP address subscriber information by administrative subpoena, but finding that defendant abandoned argument that he had reasonable expectation of privacy in IP address). In both of these cases, the Fourth Circuit found no Fourth Amendment violation. *Bynum*, 604 F.3d at 164; *Hambrick*, 2000 WL 1062039 at *2-3.

Locational Privacy

Petitioners argue that they have a reasonable expectation of privacy in IP address information subject to the Twitter Order because it could be used to track their locations in and between particular private spaces over a period of time. Doc. 45 at 20-24. Petitioners rely on *United States v. Karo*, in which the Supreme Court found a Fourth Amendment violation when the government used an electronic beeper placed in an ether can to obtain information about the inside of a house, which led to issuance of a search warrant. 468 U.S. 705, 707-10 (1984). Government agents tracked the beeper between multiple houses, determining that the ether can was inside a particular house at a particular time. *Id.* at 714. The Supreme Court found a violation of the Fourth Amendment because the beeper was monitoring the inside of a private residence which was not open to visual surveillance. *Id.* at 715. Specifically, the Court objected to the agents' use of the beeper for a significant time to determine that the ether can remained on the premises, out of view. *Id.* This usage revealed "a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." *Id.* The Court distinguished its seemingly contrary result in *United States v. Knotts*, 460 U.S. 276, 281-82 (1983) by noting that *Knotts* had involved warrantless surveillance of information that was "voluntarily conveyed to anyone who wanted to look . . ." *Karo*, 468 U.S. at 715 (quoting *Knotts*, 460 U.S. at 281). *Karo*, by contrast, involved

information in excess of what visual surveillance could have discovered.

Petitioners argue that because a person's location in a private dwelling could be revealed by IP address information collected from service providers, IP address information is analogous to the beeper device and locator in *Karo*. The government responds that *Karo* requires a warrant for using a tracking device to obtain information about the inside of a dwelling, but points out that neither the Supreme Court nor the Fourth Circuit has applied *Karo* to business records, even though such records could reveal a person's location at a particular time. Doc. 55 at 18 n.8.

Petitioners' analogy between beeper surveillance and IP address location tracking is ultimately unpersuasive. To begin with, *Karo* involved surveillance revealing information about the interior of a private home even though the tracked property had "been withdrawn from public view[.]" 468 U.S. at 714-16. Here the situation is reversed. Instead of withdrawing their IP address information from public view, Petitioners transmitted their IP address information out of any private spaces and onto the Internet. In so doing, Petitioners exposed their IP address information to all routers conveying their Internet traffic to Twitter. There is no indication that the government monitored, tracked, or otherwise conducted surveillance of private spaces using IP address information.

Moreover, the IP address records sought by the Twitter Order were recorded by Twitter, not the government. As noted before, service providers routinely keep logs of IP addresses that access their sites. Bellovin Br. at 7-8; *see also* Bringola Decl. at 22. Petitioners' use of Twitter required them to disclose their IP addresses to Twitter.[14] If Twitter decided to record or retain this information, any privacy concerns were the consequence of private action, not government

[14] Even if Petitioners were unaware that Twitter could or would record their IP addresses, or that subsequent legal process might result in disclosure, the records were created by Twitter. The inquiry here therefore focuses not on the IP address information itself, but on the propriety of using § 2703(d) to obtain IP address records from the private business that created them.

action. The mere recording of IP address information by Twitter and subsequent access by the government cannot by itself violate the Fourth Amendment. *Cf. United States v. Jacobsen*, 466 U.S. 109, 115-17 (1984) ("It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information[.]") (citing *Miller*, 425 U.S. at 443).

Petitioners and amici argue that the possibility of using IP address information to "pinpoint" a person's physical location extends to "locations in, and movements between, particular private spaces over a period of time." Doc. 45 at 20. As the government points out, however, investigators have long been able to use other forms of information to place a caller in a particular place, such as a private home, at a particular time. The Fourth Circuit has explicitly approved the collection of non-IP subscriber information for this very purpose. *See Bynum*, 604 F.3d at 164 n.2. The granularity of the "pinpoint" accuracy of IP address location finding, as described in Petitioners' brief, is hardly a function of examining IP addresses by themselves. Rather, as in the case of the commercial enterprises described by the Bellovin Brief, the granularity of the "pinpoint" information results from aggregation and correlation of IP address information with other records. Bellovin Br. at 7-8. "Pinpointing" a person's location is even more difficult if the government must distinguish between users of "static" or "dynamic" IP addresses because "dynamic" IP addresses are not consistently used by the same computer. The Court finds nothing in *Karo* or other cases indicating that combining records of IP address information with other information would infringe a locational privacy interest protected by the

Fourth Amendment.[15]

Third-Party Doctrine

Even if Petitioners had a reasonable expectation of privacy in IP address information collected by Twitter, Petitioners voluntarily relinquished any reasonable expectation of privacy under the third-party doctrine. To access Twitter, Petitioners had to disclose their IP addresses to third parties. This voluntary disclosure—built directly into the architecture of the Internet—has significant Fourth Amendment consequences under the third-party doctrine, as articulated in *United States v. Miller* and *Smith v. Maryland.*

In *United States v. Miller*, the Supreme Court addressed the use of bank records produced in response to allegedly defective subpoenas. 425 U.S. at 436. The government had obtained bank documents pursuant to defective subpoenas duces tecum issued while investigating an illegal distilling operation and used those documents for further investigation and at trial. *Id.* at 438. At trial, the defendant unsuccessfully moved to suppress the records as illegally seized under the Fourth Amendment. *Id.* at 438-39. The Supreme Court affirmed the conviction, holding that the defendant had no protectable privacy interest in the records because the records were not confidential communications, but rather negotiable instruments used in commercial transactions. *Id.* at 442. The documents obtained by the subpoena contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* The Supreme Court said that the defendant "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government, . .

[15] In support of their argument that even movement in public spaces may be protected by the Fourth Amendment, Petitioners cite the D.C. Circuit's opinion in *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010), *cert. granted*, 131 S. Ct. 3064 (2011) and the Third Circuit's opinion in *In re Application for an Order to Disclose Records (Third Circuit Opinion)*, 620 F.3d 304, 312 (3d Cir. 2010). Doc. 45 at 21. Again, the Court sees little resemblance between the tracking devices in *Maynard*, *Karo*, and *Knotts* and the retrieval of stored electronic records here. For discussion of *Third Circuit Opinion*, see *infra*.

. even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443.

Three years later, in *Smith v. Maryland*, the Supreme Court approved warrantless use of a pen register, a device which recorded the date, time, and number—but not the content—of each telephone call placed from the defendant's house. 442 U.S. at 736 n.1. The Court rejected the argument that any expectation of privacy the defendant had in the dialing of a phone number was reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. The Court specifically rejected the contention that monitoring the defendant's use of his home telephone was unacceptable because of the location used to make the phone calls:

> But the site of the call is immaterial for purposes of analysis in this case. Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

Smith, 442 U.S. at 743. In other words, the defendant in *Smith* voluntarily disclosed information to the telephone company as a necessary condition of completing his telephone call, and therefore voluntarily relinquished any rational expectation of privacy in that information. The fact that his telephone was located in his house made no difference. The Supreme Court therefore found a voluntary disclosure of information in the defendant's action of dialing the telephone:

> When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching

> equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

Id. at 744-45. The Court's holding did not depend on the company's record-keeping policies. *Id.* at 745. It was enough, the Court said, that "petitioner voluntarily conveyed to it information that it [the phone company] had facilities for recording and that it was free to record."[16] *Id.*

Like the defendant in *Smith*, Petitioners relied on Internet technology to access Twitter, indicating an intention to relinquish control of whatever information would be necessary to complete their communication. They knew that their communications with Twitter would be transmitted out of private spaces and onto the Internet for routing to Twitter. Petitioners nonetheless insist that the Internet is so unlike other communication technologies that there can be no analogy between phone numbers and IP addressing information. The Court disagrees. Both phone numbers and IP addresses must be revealed to intermediaries as a practical necessity of completing communications over their respective networks. *See Christie*, 624 F.3d at 574 ("Similarly, no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs.") (citing *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.")). Both are automatically revealed to the other party and any intermediaries carrying the communication. Both can be associated with particular persons by

[16] In fact, the SCA protects Petitioners' non-content records to a greater extent than does either *Smith* or *Miller*. In *Miller*, the Supreme Court did not disturb the lower court's finding that the subpoenas issued for the bank records were defective, and reversed primarily because of the absence of a reasonable expectation of privacy in the bank records. *Miller*, 425 U.S. at 440. Likewise, in *Smith*, the police asked the telephone company to install the pen register without a warrant or court order. *Smith*, 442 U.S. at 737.

correlation with other sources of data. Accordingly, the Court finds the analogy between phone numbers and IP addresses persuasive.

Petitioners respond that *Smith* and *Miller* are distinguishable because Petitioners did not voluntarily turn over their IP addressing information to Twitter. Doc. 45 at 21-24. They argue that because IP address information is communicated to Twitter by a web browser or other software, and is "largely hidden" from the typical user, conveyance of that information is unlike telephone numbers or bank records. They also cite the recent Third Circuit decision in *Third Circuit Opinion*, *supra* note 15, 620 F.3d at 312, 317-18, which stated that a cellular phone customer does not "voluntarily" share his cellular site location information (CSLI) with a cellular phone provider in any meaningful way.[17]

Two distinguishing factors make the Third Circuit's approach in *Third Circuit Opinion* inappropriate here. First, *Third Circuit Opinion* rejected the government's attempt to apply *Smith* and *Miller* to a location-finding device. As noted before, no such technology is implicated in this matter. *Karo* belongs to a different line of cases and is inapplicable on its face. Second, there is no indication that the cellular technology in *Third Circuit Opinion* required location information from a cellular phone as a practical necessity of completing cellular communications. IP addresses, by contrast, are a fundamental part of the Internet's architecture, and cannot be eliminated from Internet communication without rendering the technology useless. They can be masked or obfuscated by using intermediary computers, but the IP address information itself is a functional necessity. Petitioners communicated their IP addresses to Twitter by using Internet-connected devices to access their accounts, demonstrating voluntary assent to whatever disclosures would be necessary to complete the communications. *See* Doc. 55 at 19-22. In this

[17] Though the Third Circuit did not have a factual record before it on appeal, 620 F.3d at 312, it postulated that most users are unaware that cellular phone providers collect or store historical location information. *Id.* at 317-18.

respect, the Internet provides less privacy to IP addresses than the telephone network did for telephone numbers. Before cellular telephones became vastly more popular it was the exception, not the rule, for a wired telephone to reveal the number of an incoming caller. For Internet communications, by contrast, IP address disclosure must occur. The fact that a particular user may not see or know which IP address he is using at a particular moment does not create a reasonable expectation of privacy in the information. If the user is communicating over the Internet, intermediary computers and the destination computer must know the IP address as a condition of communication. Under the Fourth Amendment, that fact renders unreasonable any expectation of privacy in the IP address.

Petitioners retort that they, as Twitter users, were not "explicitly notified" that Twitter collects IP addresses, and that anyway, most users do not read privacy policies for Internet sites they visit. Doc. 45 at 24. This merits three responses. First, as already noted, Petitioners voluntarily chose to use Internet technology to communicate with Twitter and thereby consented to whatever disclosures would be necessary to complete their communications.

Second, as Petitioners conceded at the hearing before Magistrate Judge Buchanan on February 15, 2011, indicating acceptance of Twitter's Privacy Policy was a condition of creating a Twitter account. Doc. 41 at 17:1-6. No party disputes that the Privacy Policy permits Twitter to retain Petitioners' IP address information.[18] Petitioners argue that the provision of the Privacy Policy covering IP addresses was not "immediately apparent to users" and that the policy would only put Twitter customers on notice "if accessed and read." Doc. 45 at 24. These considerations are not irrelevant, but they do not prevail here. Regardless of whether the Privacy Policy binds Petitioners in contract, an issue not presented, Petitioners' apparent willingness to provide their

[18] The Privacy Policy also clearly contemplates the communication and retention of location-based information. Doc. 45-1 at 22-23.

information to Twitter—with or without reading Twitter's policies—weighs in favor of a finding that Petitioners voluntarily revealed their IP address information to Twitter. The Court looks at all of the evidence to determine whether Petitioners voluntarily submitted their information Twitter, and on the evidence presented, it is clear that they did so.[19] *See Florida v. Jimineo*, 500 U.S. 248, 251 (1991) (standard of subject's consent is objective reasonableness); *United States v. Bullard*, 645 F.3d 237, 242 (4th Cir. 2011) (expectation of privacy must be objectively reasonable); *United States v. Coleman*, 588 F.3d 816, 819 (4th Cir. 2009) (objective reasonableness standard for measuring suspect's consent); *United States v. Buckner*, 473 F.3d 551, 555-56 (4th Cir. 2007) (objective reasonableness); *United States v. Wheatland*, 57 Fed. Appx. 194, 195 (4th Cir. 2003) (voluntariness of consent involves objective analysis of the totality of circumstances).

Petitioners' additional citations to *United States v. Warshak*, 631 F.3d 266, 286-88 (6th Cir. 2010) and *United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) are also distinguishable. *Warshak* does not apply because it disapproved of a § 2703 order seeking *contents* of the defendant's emails, whereas the Twitter Order sought only non-content *records* of Petitioners' Twitter usage. *Warshak*, 631 F.3d at 282. *Heckenkamp* is likewise inapposite because the intrusion at issue was a remote search of the defendant's computer, which included running commands and examining files stored on the defendant's personal computer. *Heckenkamp*, 482 F.3d at 1144-45. Personal computers are ordinarily treated like closed containers under the Fourth Amendment, and different analysis applies. *See generally* U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal*

[19] The Court likewise considers it improbable that two of the Petitioners, who are computer security experts, were subjectively unaware of the possibility of IP address logging or the possibility that someone could use their IP addresses to estimate their geographical locations.

Investigations 3-10 (2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf. Furthermore, unlike either *Warshak* or *Heckenkamp*, this matter is governed by the third-party doctrine as set forth in *Smith* and *Miller*.

Another Third Circuit case cited by the government, *United States v. Christie*, is on point. 624 F.3d at 558. *Christie* held that users do not have a reasonable expectation of privacy in IP address records because IP address information is "subscriber information provided to an Internet provider." 624 F.3d at 573-74 (citing *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008); *Bynum*, 604 F.3d at 164). As the Third Circuit observed there, "no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs. IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *Christie*, 624 F.3d at 574 (citations and quotations omitted) (citing *Forrester*, 512 F.3d at 510).

In addition, Petitioners challenge Magistrate Judge Buchanan's partial reliance on *United States v. Forrester*, *supra*, a Ninth Circuit case involving the use of court-approved computer surveillance that revealed the source and destination IP addresses of websites visited by the defendant. 512 F.3d at 504-05, 510; Doc. 45 at 23. The court there held that the surveillance technology was the equivalent of the pen registers in *Smith*, and that its use did not constitute a search. *Id.* at 509-10. Petitioners distinguish *Forrester* by arguing that the IP addressing information there was used only for routing of IP packets, whereas here "Twitter's IP logs serve no such purpose." Doc. 45 at 23. The two propositions, however, are not mutually exclusive. As in *Forrester*, IP addresses were necessary to route Petitioners' communications to Twitter over the Internet. This is true of all Internet communications. The fact that Twitter chose to record IP

address information pertaining to Petitioners, and the purpose for which it did so, makes no difference. *Forrester* is precisely on point in this respect. As the Supreme Court stated in *Smith*, the meaning of the Fourth Amendment cannot be dictated by the record-keeping practices of a private corporation. *Smith*, 442 U.S. at 745 ("We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.").

Petitioners' attempt to distinguish *Forrester* in this way also overlooks the Ninth Circuit's observation that Internet users "should know that [IP address] information is provided to and used by Internet service providers for the specific purpose of directing the routing of information" because they "are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *Forrester*, 512 F.3d at 510. Petitioners argue that the IP address information sought here is different because it reveals their real-world movements, and therefore implicates locational privacy concerns. Doc. 45 at 23. Even accepting that premise *arguendo*, IP addressing information is not immune to voluntary disclosure under the third-party doctrine. *See Forrester*, 512 F.3d at 510. IP addresses are no more revealing about the contents of communication than are phone numbers. *Id.* As with phone numbers, government agents collecting IP address information from a communications channel may be able to make educated guesses about what was said, simply based on non-content information about the parties involved in the communication. *Id.* Yet in *Smith*, the Supreme Court drew a "clear line between unprotected addressing information and protected content information[.]" *Id.* The Twitter Order was far less intrusive than the real-time surveillance of non-content information approved in *Forrester*. *See id.* at 511. Magistrate Judge Buchanan was therefore correct to rely on the Ninth Circuit's reasoning.

Two consequences follow from the Court's conclusion that Petitioners voluntarily relinquished any expectation of privacy in their IP addressing information when they chose to use the Internet to communicate with the Twitter service. First, because the Twitter Order did not invade Petitioners' reasonable expectations of privacy, it cannot constitute a search in violation of the Fourth Amendment. *See Florida v. Riley*, 488 U.S. 445, 449-50 (1989); *California v. Ciraolo*, 476 U.S. 207, 211 (1986) ("The touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'") (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring)). Therefore their Fourth Amendment challenge to the Twitter Order fails.

Second, Petitioners do not have Fourth Amendment standing to object to the Twitter Order. They have not alleged a personal injury cognizable by the Fourth Amendment, nor have they been charged with any substantive offense based on information obtained as a result of the Twitter Order. No personal injury fairly traceable to the allegedly unlawful conduct has therefore been shown. *See Cty. of Riverside v. McLaughlin*, 500 U.S. 44, 51 (1991); *cf. Karo*, 468 U.S. at 721 ("Because locating the ether in the warehouse was not an illegal search—and because the ether was seen being loaded into Horton's truck, which then traveled the public highways—it is evident that under *Knotts* there was no violation of the Fourth Amendment as to anyone with or without standing to complain about monitoring the beeper while it was located in Horton's truck."); *Rawlings v. Kentucky*, 448 U.S. 98, 104-05 (1980); *Rakas v. Illinois*, 439 U.S. 128, 148-50 (1978). Without a reasonable expectation of privacy in the subject information, therefore, Petitioners are not entitled to challenge the Twitter Order on Fourth Amendment grounds. *Cf. Rakas*, 439 U.S. at 149-50; *Rawlings*, 448 U.S. at 105-06.

(II) Scope of the Twitter Order

Even if Petitioners retained a reasonable expectation of privacy in IP address information, Petitioners' Fourth Amendment challenge cannot succeed without also proving that the Twitter Order was unreasonable under the Fourth Amendment. *See City of Ontario, Cal. v. Quon*, --- U.S. ---, 130 S. Ct. 2619, 2629 (2010) (assuming but not affirming the existence of a reasonable expectation of privacy for Fourth Amendment analysis). The Twitter Order sought only information from a particular time period that was specifically authorized by the SCA, and the order sought no content information. Petitioners knew or should have known that their IP address information was subject to examination by Twitter, so they had a lessened expectation of privacy in that information, particularly in light of their apparent consent to the Twitter Terms of Service and Privacy Policy. *Cf. Wyoming v. Houghton*, 526 U.S. 295, 303-06 (1999) (lessened expectation of privacy in property transported by automobiles, which "travel public thoroughfares, seldom serve as the repository of personal effects, are subjected to police stop and examination to enforce pervasive governmental controls as an everyday occurrence, and, finally, are exposed to traffic accidents that may render all their contents open to public scrutiny." (citations, ellipses and quotations omitted)). They also implicitly consented to disclosure of their IP address information to Twitter as a practical necessity of using Internet technology. The Court therefore concludes that even if Petitioners had a reasonable expectation of privacy in their IP address information, the Twitter Order was not intrusive and was, in fact, reasonable.[20]

[20] The Court must note two pertinent differences between *Quon* and this case. First, *Quon* involved a search of the contents of the plaintiff's text messages. Here, the Twitter Order sought only non-content records. Second, *Quon* did not address the precise contours of the assumed reasonable expectation of privacy. Petitioners have challenged only the disclosure of IP address information here, so the Court need only address whether the disclosure of IP address information is unreasonable.

3. Due Process

The next issue is whether Petitioners have a constitutional right to challenge the Twitter Order under the Due Process Clause. Magistrate Judge Buchanan held that they had no such right. Petitioners argue that without a pre-execution opportunity to challenge an order issued under § 2703, the SCA threatens the rights of any subscriber who cannot oppose an order because the individual does not know about it. They do not allege that a violation of the SCA resulted in infringement of their Due Process rights, only that they have a constitutional Due Process right to challenge the § 2703 order at this time. The Court therefore concludes that Petitioners base their argument on procedural due process.

Petitioners cite only one relevant due process case, *Mathews v. Eldridge*, 424 U.S. 319, 333 (1976).[21] In *Mathews*, the Supreme Court overturned the district court's decision to enjoin termination of the plaintiff's Social Security disability benefits. The district court determined that the administrative procedures governing revocation of the plaintiff's disability benefits were constitutionally inadequate, but the Supreme Court disagreed. In describing its approach to the petitioner's procedural due process claim, the Supreme Court explained its now oft-cited test for procedural due process claims:

> [O]ur prior decisions indicate that identification of the specific dictates of due process generally requires consideration of three

[21] Petitioners cite a D.C. Circuit opinion, *Rafeedie v. INS*, 880 F.2d 506 (D.C. Cir. 1989), which addresses procedures for exclusions under the Immigration and Nationality Act. The interests affected by a § 2703 order are vastly different than those affected by exclusion or deportation. Petitioners also cite *Eastland v. U.S. Serviceman's Fund*, 421 U.S. 491, 501 n.14 (1975) for the proposition that courts have "long recognized" a right to challenge disclosure demands that raise constitutional issues. Doc. 45 at 13. The Court declines to accept such a broad reading of *Eastland*. *Eastland* involved a congressional subpoena to a private bank for records of a subject organization, and the subject organization filed an action to enjoin enforcement of the subpoena. *Eastland*, 421 U.S. at 494-97. The similarity between this case and *Eastland* ends there. *Eastland* addressed Congress's legislative power to investigate, an issue having no application to this case and far removed from the rather typical context of this investigation. Moreover, the SCA provides for either a post-execution review of a § 2703(d) order through a civil action or administrative proceeding or a quashal proceeding instituted by the service provider. *Eastland*'s concern that some party have a plausible reason or opportunity to resist a subpoena to a third party is absent here. *See* 18 U.S.C. § 2707(d).

> distinct factors: First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.

Mathews, 424 U.S. at 334-35. Though sometimes urged in support of an as-applied challenge, *Mathews* requires the Court to analyze the procedure in question as it relates to the run-of-the-mill case. *Walters v. Nat'l Ass'n of Radiation Survivors*, 473 U.S. 305, 330 (1985).

The Supreme Court has never announced *Mathews* as an all-embracing test for deciding due process claims, however. *Dusenberry v. United States*, 534 U.S. 161, 168 (2002) ("Although we have since invoked *Mathews* to evaluate due process claims in other contexts, we have never viewed *Mathews* as announcing an all-embracing test for deciding due process claims." (citations omitted)). To the contrary, the Supreme Court has explained that the Fourth Amendment is adequate to protect procedural rights in certain types of criminal proceedings:

> *Gerstein* [*v. Pugh*, 420 U.S. 103 (1975)] held that the Fourth Amendment, rather than the Due Process Clause, determines the requisite post-arrest proceedings when individuals are detained on criminal charges. Exclusive reliance on the Fourth Amendment is appropriate in the arrest context, we explained, because the Amendment was tailored explicitly for the criminal justice system, and its balance between individual and public interests always has been thought to define the process that is due for seizures of person or property in criminal cases. Furthermore, we noted that the protections afforded during an arrest and initial detention are only the first stage of an elaborate system, unique in jurisprudence, designed to safeguard the rights of those accused of criminal conduct.
>
> So too, in *Graham* [*v. Connor*, 490 U.S. 386 (1989)] we held that claims of excessive force in the course of an arrest or investigatory stop should be evaluated under the Fourth Amendment reasonableness standard, not under the more generalized notion of "substantive due process." Because the degree of force used to effect a seizure is one determinant of its reasonableness, and

> because the Fourth Amendment guarantees citizens the right "to be secure in their persons ... against unreasonable ... seizures," we held that a claim of excessive force in the course of such a seizure is most properly characterized as one invoking the protections of the Fourth Amendment.

United States v. James Daniel Good Real Property, 510 U.S. 43, 50-51 (1993) (citations and quotations omitted). Whether the Due Process Clause applies to a particular seizure typically depends on the purpose of the seizure. *Id.* at 51-52. For example, if the government seizes property "not to preserve evidence of wrongdoing, but to assert ownership and control over the property itself," as in a forfeiture proceeding, the Due Process Clause analysis provides additional protection beyond that afforded by the Fourth Amendment. *See id.* If the government seizes property to preserve evidence of wrongdoing, by contrast, only the Fourth Amendment applies. *Id.* In such circumstances, the Fourth Amendment resolves the legality of governmental action "without reference to other constitutional provisions." *Id.* at 51. If the Fourth Amendment were sufficient to resolve the matter before the Court, for example, the finding that Petitioners lacked a reasonable expectation of privacy would be dispositive.

In other cases, the Supreme Court has turned to the Fourth Amendment to evaluate challenges to subpoenas issued by a grand jury. *See, e.g.*, *United States v. Calandra*, 414 U.S. 338, 346 (1974) ("The grand jury is also without power to invade a legitimate privacy interest protected by the Fourth Amendment. A grand jury's subpoena duces tecum will be disallowed if it is far too sweeping in its terms to be regarded as reasonable under the Fourth Amendment. Judicial supervision is properly exercised in such cases to prevent the wrong before it occurs." (citations and quotations omitted)); *United States v. Dionisio*, 410 U.S. 1, 11-12 (1973) (citing *Hale v. Henkel*, 201 U.S. 43, 76 (1906), *overruled on other grounds by Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 65-73 (1964)).

Ultimately, the Court need not address here whether the Fourth Amendment subsumes the protections provided by the Due Process clause because § 2703(d) survives scrutiny under *Mathews*. "The fundamental requirement of due process is the opportunity to be heard at a meaningful time and in a meaningful manner." *Mathews*, 424 U.S. at 333 (quotations omitted). Assuming *arguendo* that the Twitter Order implicates an interest protected by the Due Process clause,[22] the SCA already reduces the risk of erroneous deprivation of that interest through pre-issuance judicial review of all § 2703 orders, and special notice and hearing opportunities under certain circumstances. 18 U.S.C. §§ 2703-04. Any executive actors who violate the Constitution under § 2703 are subject to civil or administrative action, or perhaps a *Bivens* action (though the Court expresses no opinion on that issue). *See* 18 U.S.C. § 2707(d). Petitioners presumably could litigate each and every one of their claims in a pretrial motion if they became subjects of a prosecution. In short, Petitioners have identified no way in which relief would be unavailable at a post-execution hearing.

In light of the principle set forth in *Mathews* that "[a] claim to a predeprivation hearing as a matter of constitutional right rests on the proposition that full relief cannot be obtained at a postdeprivation hearing," *Mathews*, 424 U.S. at 331, the Court concludes that no pre-execution hearing is necessary here. Though affording subjects like Petitioners the routine opportunity to challenge a § 2703 order prior to its execution could, theoretically, provide some incremental improvement of the § 2703 process, it would thoroughly trivialize the role that judicial oversight already provides. *See Walters*, 473 U.S. at 320-21 ("In defining the process necessary to ensure 'fundamental fairness' we have recognized that the [Due Process] Clause does not require that

[22] Though the seizure cases under the Due Process Clause involve clear possessory interests in property, there is good reason to believe that Petitioners here have no interest protected by the Due Process Clause. As explained *supra*, the Fourth Amendment does not protect information in which a party has no reasonable expectation of privacy, in this case, under the third-party doctrine.

the procedures used to guard against an erroneous deprivation be so comprehensive as to preclude any possibility of error, and in addition we have emphasized that the marginal gains from affording an additional procedural safeguard often may be outweighed by the societal cost of providing such a safeguard." (citations omitted)).

Under the SCA, the government can obtain a § 2703 order only after approval by an impartial judicial officer. The facts supporting the issuance of an order must satisfy constitutional and statutory standards. Issuing a § 2703 order affects none of the subject's protected interests, such as life, liberty, or property, nor is there any guarantee that formal charges will follow from evidence obtained through such an order. Formal charges are subject to typical procedural requirements for criminal cases, such as indictment requirements and probable cause. Because the SCA is typically invoked in preliminary proceedings, not proceedings finally affecting substantive rights, the SCA strikes a balance between the government's need for prompt access to evidence and the limited privacy interest in information sought under the § 2703 order.

The Court is also wary of depriving the grand jury of information that it would find relevant and material to its investigation. The Supreme Court has described the grand jury as "the sole method for preferring charges in serious criminal cases." *Branzburg v. Hayes*, 408 U.S. 665, 687 (1972) (quoting *Costello v. United States*, 350 U.S. 359, 362 (1956)). "It is a grand inquest, a body with powers of investigation and inquisition, the scope of whose inquiries is not to be limited narrowly by questions of propriety or forecasts of the probable result of the investigation, or by doubts whether any particular individual will be found properly subject to an accusation of crime." *Id.* at 688 (citing *Blair v. United States*, 250 U.S. 273, 282 (1919)). The investigative powers of the grand jury are "necessarily broad," and "the grand jury's authority to subpoena witnesses is not only historic, but essential to its task." *Id.* at 688 (citations omitted). To the

extent that Petitioners' argument would hinder the grand jury in its task of obtaining relevant information, it must be carefully scrutinized.

Moreover, allowing routine challenges of § 2703 orders would undermine grand jury secrecy, which helps maintain the integrity of the grand jury's function. *See United States v. Williams*, 504 U.S. 36, 48 (1992); Fed. R. Crim. P. 6(e). As the Supreme Court has observed:

> We consistently have recognized that the proper functioning of our grand jury system depends upon the secrecy of grand jury proceedings. In particular, we have noted several distinct interests served by safeguarding the confidentiality of grand jury proceedings. First, if preindictment proceedings were made public, many prospective witnesses would be hesitant to come forward voluntarily, knowing that those against whom they testify would be aware of that testimony. Moreover, witnesses who appeared before the grand jury would be less likely to testify fully and frankly, as they would be open to retribution as well as to inducements. There also would be the risk that those about to be indicted would flee, or would try to influence individual grand jurors to vote against indictment. Finally, by preserving the secrecy of the proceedings, we assure that persons who are accused but exonerated by the grand jury will not be held up to public ridicule.

Douglas Oil Co. of California v. Petrol Stops Northwest, 441 U.S. 211, 218-19 (1979) (citations omitted); *see also United States v. Procter & Gamble Co.*, 356 U.S. 677, 681-82 n.6 (1958) (approving Third Circuit's explanation for grand jury secrecy, encouraging "free and untrammeled disclosures by persons who have information with respect to the commission of crimes"). "Although the purpose for grand jury secrecy originally was protection of the criminally accused against an overreaching Crown, with time it came to be viewed as necessary for the proper functioning of the grand jury." *See Douglas Oil*, 441 U.S. at 219 n.9.

Other factors weigh in favor of secrecy. As a brief examination of the Twitter Order makes clear, it is rather easy to guess the probable subject matter and targets of the otherwise secret grand jury investigation by reviewing associated legal process. Even where the

government does not consent to unsealing of a § 2703 order, as it did here, requiring pre-execution notice and opportunity to object to all subjects of § 2703 orders would vastly decrease the grand jury's ability to carry on its constitutional function. The effects of such a general rule would be catastrophic.

The peculiar nature of electronic data is a further consideration. Electronic evidence poses an even greater danger of destruction or concealment than does traditional physical evidence. As the courts are discovering, electronic evidence can be overwritten, transferred, or expunged with little to no human effort, and if performed by a competent expert, may leave little trace that it ever existed. *See, e.g.*, *Zubulake v. UBS Warburg LLC* (*Zubulake IV*), 220 F.R.D. 212, 214, 214 n.2 (S.D.N.Y. 2003). Surprise in the execution of a § 2703 order may therefore be even more important than speed. What the Supreme Court has said about search warrants is especially true of § 2703 orders: "The danger is all too obvious that a criminal will destroy or hide evidence or fruits of his crime if given any prior notice." *Calero-Toledo v. Pearson Yacht Leasing Co.*, 416 U.S. 663, 679 n.14 (1974) (affirming post-seizure notice and hearing in civil forfeiture action). In this respect, § 2703 orders are more like search warrants than grand jury subpoenas. *Cf. In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000) (discussing practical distinctions between search warrant and grand jury subpoena).

Finally, the grand jury provides Petitioners—and all other persons—with ample procedural protection. The grand jury's function in our system of criminal justice is two-fold: the grand jury returns indictments based on probable cause, and protects citizens from unfounded criminal prosecutions. *Branzburg*, 408 U.S. at 686-87; *see also Fed. Deposit Ins. Corp. v. Mallen*, 486 U.S. 230, 244 (1988) ("Moreover, and perhaps most significantly, there is little likelihood that the deprivation is without basis. The returning of the indictment establishes that

an independent body has determined that there is probable cause to believe that the officer has committed a crime punishable by imprisonment for a term in excess of one year."). The grand jury system is judicially supervised. *Branzburg*, 408 U.S. at 688. The process for issuing § 2703 orders like the Twitter Order is thus doubly protected: a judicial officer supervises the issuance of the § 2703 order, and the grand jury protects Petitioners from unjustified criminal charges.[23]

Returning to the case at hand, the Court concludes that the Due Process Clause is not violated by execution of a § 2703 order. To begin, no measurable improvement would result from further review of this type of proceeding. The SCA already provides for judicial review of applications, and Petitioners indicate no further systemic benefits that would emerge from re-examination at this point. The procedure set forth in § 2703 closely resembles the process for search warrants under the Federal Rules of Criminal Procedure, which mandate judicial supervision of applications for issuance of subpoenas, arrest warrants, and other pretrial criminal orders. *See* Fed. R. Crim. P. 41(e). Judicial supervision at this stage, even when carried out *ex parte*, provides adequate protection for subjects of § 2703 orders and ensures that any authorized incursions into protected areas will be carefully circumscribed.

Moreover, accepting the proposition that a subject of a § 2703 order is entitled to a pre-execution hearing would transform government investigations into a battle for control. In short, the Court is not persuaded that the Due Process Clause provides subjects of § 2703 orders with a generalized right to notice and opportunity to object. Judicial review and the grand jury provide Petitioners and others with procedural protections sufficient to survive constitutional scrutiny.

Finally, Petitioners object to the SCA's authorization of *ex parte* proceedings for § 2703

[23] The Supreme Court has recognized the grand jury's functional independence from the Judicial Branch of government "both in the scope of its power to investigate criminal wrongdoing and in the manner in which that power is exercised." *United States v. Williams*, 504 U.S. 36, 48 (1992) (distinguishing grand jury from courts).

orders. Doc. 45 at 30. One-sided factual determinations may be disfavored in our adversarial system, but the Constitution permits *ex parte* proceedings when they will preserve the integrity of government investigations. Grand juries, search warrants, wiretap orders, and many other *ex parte* applications and orders rely on judicial review to protect the rights of potential subjects of investigation. All of these tools have been routinely and consistently approved by the courts. In short, Petitioners have no right to challenge the issuance of a § 2703 order under the Due Process Clause, and Petitioners' argument on this point fails.

4. First Amendment

Petitioners object that the Twitter Order violates their First Amendment rights of speech and association. Doc. 45 at 17-20. They argue that the Twitter Order has chilled their rights of association and speech, and therefore the government must show "a substantial relation between the information sought and a subject of overriding and compelling state interest." Doc. 45 at 18 (quoting *Gibson v. Fla. Legislative Invest. Comm.*, 372 U.S. 539, 546 (1963)). Petitioners argue that the violations took three forms. First, they argue that because the Twitter Order sought "private" information, it has a "chilling effect" on their speech and associational rights, as well as the rights of Twitter users in general and the Twitter users who "follow" Petitioners on Twitter. Doc. 45 at 17-18. Second, they argue that the Twitter Order sought "private IP address information and other details" for Twitter messages that had nothing to do with Wikileaks and therefore were too broad to survive First Amendment scrutiny. Doc. 45 at 19. Third, Petitioners argue that the Twitter Order was unacceptable because the government has expressed a desire, as Petitioners put it, "to prosecute somebody associated with it." Doc. 45 at 19-20.

The government responds that, as Magistrate Judge Buchanan held below, Petitioners had voluntarily made their Twitter posts and associations with Wikileaks public. Doc. 55 at 12.

Consequently, any "chilling effect" of the Twitter Order could be no more severe than that created by Petitioners' own actions. Magistrate Judge Buchanan found that the government had a legitimate interest in the records, that the Twitter Order was reasonable in scope, and that the order did not seek content. Doc. 55 at 12. The government also argues that production of non-content records does not implicate First Amendment rights because such documents are obtainable by a grand jury and not "specially insulated" from investigative scrutiny. Doc. 55 at 13-14.

Petitioners cite several cases far afield from the present case.[24] *NAACP v. Button*, 371 U.S. 415 (1963) addressed a threat of sanctions against the NAACP for advising prospective litigants to seek the assistance of particular attorneys. No sanctions against Petitioners or purportedly improper legal advice are at issue here. Two of Petitioners' cases concern compelled disclosure of private membership lists. *Gibson v. Florida Leg. Investigative Comm.*, 372 U.S. 539 (1963), for example, concerned compelled disclosure of the NAACP's membership lists to a legislative investigation, not disclosure of records collected and maintained by a service provider. In *In re First Nat'l Bank*, 701 F.2d 115, 119 (10th Cir. 1983), the Tenth Circuit found a prima facie case of violation of the First Amendment where known members of the petitioner's organization had undergone harassment and intimidation and release of subpoenaed information would have inevitably disclosed the identities of still more members of the organization. *Id.* at 116-17. No membership lists were sought by the Twitter Order, nor have Petitioners introduced any evidence that harassment or intimidation has occurred. Moreover, Petitioners challenged the

[24] *N. Carolina Right to Life, Inc. v. Bartlett*, 168 F.3d 705 (4th Cir. 1999) is relevant only to the extent that chilling effects confer standing to challenge a First Amendment violation. Because no chilling effect has been demonstrated or plausibly argued, the Court finds it likely (but need not hold) that Petitioners have no First Amendment standing to challenge the Twitter Order.

Twitter Order publicly, and have thereby voluntarily disclosed that there may be some association between them and Wikileaks.

Petitioners also cite *In re Grand Jury Subpoenas Duces Tecum*, 78 F.3d 1307, 1312-13 (8th Cir. 1996), in which Independent Counsel obtained a grand jury subpoena seeking information about political contributions by persons having a financial relationship with President William Jefferson Clinton or First Lady Hillary Rodham Clinton. The subjects of the subpoena challenged the subpoena and appealed to the Eighth Circuit. The court held that even if the parties had made out a violation of their First Amendment rights (which the court assumed *arguendo*), the government had demonstrated a compelling interest in and sufficient nexus between the information sought and the subject matter of the investigation. *Id.* Here, by contrast, Petitioners have not shown that their First Amendment right of association has been impinged. Thus, the Court need not determine what test applies to the Twitter Order or whether the Twitter Order complies with *Branzburg v. Hayes*, 408 U.S. at 680-81 and *In re Grand Jury Subpoena Duces Tecum*, 955 F.2d 229, 232-34 (4th Cir. 1992).

5. Exercising Discretion to Avoid Constitutional Questions

Petitioners argue that the Court has the discretion to deny an application for a § 2703 order, and that it should use that discretion here to avoid addressing constitutional questions raised by the Twitter Order. Doc. 45 at 16. The government argues that the language of § 2703(d) forecloses the conclusion that it grants discretion to a judicial officer. Doc. 55 at 10-11. The Court concludes that the SCA does not permit discretion to decline to issue an otherwise satisfactory § 2703 order. Magistrate Judge Buchanan properly declined to vacate the Twitter Order.

Section 2703(d) states, in relevant part:

> (d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. . . .

18 U.S.C. § 2703(d).

Petitioners cite *Third Circuit Opinion*, *supra*, where the Third Circuit concluded that a magistrate judge has discretion to require the government to show that it has probable cause supporting its application before issuing a § 2703 order for records. 620 F.3d at 319. The government responds that *Third Circuit Opinion* was incorrectly decided because the Third Circuit's holding renders superfluous the phrase "and shall issue" in § 2703(d). Doc. 55 at 11. A proper reading of that statute, the government contends, would give meaning to all words in the statute, namely, requiring the magistrate to issue a § 2703 order when the application satisfies the factual burden. Doc. 55 at 11.

The government has the better argument. To begin with, § 2703 grants the power at issue to "a governmental entity," not to the judicial officer responsible for evaluating the application. *See* 18 U.S.C. § 2711(4) (defining "governmental entity" as "a department or agency of the United States or any State or political subdivision thereof"). Specifically, it is the "governmental entity" that may require disclosure of information, and it is the burden of the "governmental entity" to show facts supporting the application. *See* 18 U.S.C. § 2703(c)(1). The statute contemplates a simple situation in which the government presents its application for review by a judicial officer, who either approves or denies it.

In *Third Circuit Opinion*, the government had taken the position that § 2703(c) allows it

to pick between several methods of obtaining disclosure of electronic information. The Third Circuit was unpersuaded by the government's explanation for why § 2703(c) would give such discretion to the government. Section 2703 states that "A governmental entity may require" disclosure of records "only when the governmental entity" goes through the normal warrant process, obtains a § 2703 order, obtains subscriber or customer consent, submits a formal written request related to a telemarketing fraud investigation, or uses an administrative, grand jury, or trial subpoena. *See* 18 U.S.C. § 2703(c). It was unclear to the Third Circuit why § 2703(c)(1)(A) would permit the government the option to seek a warrant based on probable cause when it could also obtain a § 2703 order with a lower evidentiary showing. *Third Circuit Opinion*, 620 F.3d at 316.

The Court believes the reason has been cogently articulated by Professor Kerr:

> The main reason is efficiency. Investigators may decide that they need to compel several types of information, some of which can be obtained with lesser process and some of which requires greater process. The 'greater includes the lesser' rule in § 2703 allows the government to obtain only one court order—whatever process is greatest—and compel all of the information in one order all at once.

Kerr, *supra*, at 1220, 1222; *see In re Application of the United States for an Order Authorizing Installation and Use of a Pen Register*, 441 F. Supp. 2d 816, 829 (S.D. Tex. 2006); *cf. United States v. N.Y. Tel. Co.*, 434 U.S. 159, 170 (1977) ("Indeed, it would be anomalous to permit the recording of conversations by means of electronic surveillance while prohibiting the far lesser intrusion accomplished by pen registers. Congress intended no such result."). Congress could permit the government to seek disclosure of records under a variety of circumstances with appropriate factual burdens, and the Court sees no reason to substitute judicial discretion for congressionally-selected options.

The Third Circuit also held that § 2703(d) was permissive because it established that "[a]

court order for disclosure under subsection (b) or (c) *may* be issued by any court that is a court of competent jurisdiction and *shall* issue only if" the statutory requirements were met. 18 U.S.C. § 2703(d) (emphasis added). In the Third Circuit's view, the "may issue" language granted discretion to the judicial officer, while the "shall issue only if" language described an additional necessary but not necessarily sufficient condition of issuance. *Third Circuit Opinion*, 620 F.3d at 315-16. In light of the permissive language of § 2703(d), the Third Circuit considered it more likely that Congress intended that the magistrate judge require different levels of proof for each method of disclosure and held that the magistrate had discretion to require a warrant, though it should "be used sparingly." *Id.* at 318-19.

On a grammatical level, the Third Circuit's interpretation incorrectly treats the phrase "may be issued" as if it governs the rest of the first sentence of § 2703(d), when in fact it governs only the first independent clause of the first sentence. 18 U.S.C. § 2703(d). The provision that the order "may be issued" is enabling language that allows the government to seek an order in any court of competent jurisdiction. The next sentence in the paragraph confirms that "may be issued" governs the question of who can issue the order because "and shall issue only if" establishes the appropriate action once the government has satisfied its factual predicate. Moreover, the fact that a state governmental authority "shall not issue" an order when state law forbids it makes clear that the default rule is issuance. When viewed in this way, it is clear that the general rule is that the judicial officer "shall issue" an order that meets the factual burden.

Petitioners argue, as did the Third Circuit, that this does not end the inquiry because the phrase includes the words "only if." The Third Circuit relied on a prior case holding that the phrase "only if" established a necessary but not sufficient condition. *Third Circuit Opinion*, 620 F.3d at 316. The Court agrees that "only if" serves that function here. The fact that "only if"

creates a necessary but not sufficient condition, however, does not automatically create a gap in the statute that should be filled with judicial discretion. The Court considers it more likely that the "only if" language in § 2703(d) clarifies that any conditions established by (b) and (c) are cumulative with respect to the standard set forth in paragraph (d). The default rule remains that the judicial officer "shall issue" an order when the government meets its burden.

Petitioners' argument that constitutional avoidance requires the exercise of discretion to vacate the Twitter Order likewise fails. Because Petitioners have not demonstrated that the Twitter Order poses constitutional problems, or that Magistrate Judge Buchanan had discretion to refuse issuance of the Twitter Order, the Court need not address the propriety of constitutional avoidance.

6. Other Issues

Petitioners did not object to Magistrate Judge Buchanan's finding that international comity does not justify vacatur of the Twitter Order as to Ms. Jonsdottir, and the Court will not disturb that conclusion here. In addition, the Twitter Order did not violate the Constitution, and Petitioners point to no authority conferring additional non-constitutional protections upon Ms. Jonsdottir. The Court therefore need not address extraterritorial application of the Constitution.

C. Motion to Unseal

Petitioners moved for unsealing and for public docketing under the First Amendment, the Due Process Clause, and the common law right of access to court records. Magistrate Judge Buchanan granted the motion in part and denied it in part. She granted their motion insofar as it applied to documents filed in the matter having docket number 1:11-dm-3, which had been created as a special docket number to organize the events in this matter, but denied it in all other respects. Petitioners now object to Magistrate Judge Buchanan's denial of their motion for

unsealing of all documents related to the Twitter Order, and their motion for public docketing of all § 2703 orders relating to Petitioners in the matter under investigation. Doc. 45 at 25-36; Doc. 64 at 11-27.

1. First Amendment

Petitioners contend that Magistrate Judge Buchanan applied the wrong standard in determining that they have no First Amendment right of access. Doc. 45 at 25-26. They argue that she improperly weighed the need for secrecy against their own interest and the public interest, and that unsealing of the Twitter Order eliminates any justification for further sealing. Doc. 45 at 28-32. They also argue that the government does not have an interest sufficient to justify sealing and that Magistrate Judge Buchanan failed to consider adequate alternatives to sealing. Doc. 45 at 32-36.

The First Amendment allows a public right of access where (1) the place and process to which access is sought has historically been open to the press and general public; and (2) public access plays a significant positive role in the functioning of the particular process. *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 64 (4th Cir. 1989) (citing *Press-Enterprise Co. v. Superior Court (Press-Enterprise II)*, 478 U.S. 1, 8-10 (1986)). To date, First Amendment public access rights have been extended to many aspects of the criminal process. *See Presley v. Georgia*, --- U.S. ---, 130 S. Ct. 721, 724 (2010) (voir dire); *Butterworth v. Smith*, 494 U.S. 624, 635-36 (1990) (witness's own grand jury testimony); *Press-Enterprise II*, 478 U.S. at 13-15; *Press-Enterprise Co. v. Superior Court (Press-Enterprise I)*, 464 U.S. 501, 511 (1984); *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, (1982) (some aspects of criminal trials); *In re Washington Post Co.*, 807 F.2d 383, 390 (4th Cir. 1986) (plea and sentencing hearings in criminal cases).

Petitioners argue that where there is no centuries-old history of openness upon which to

draw, such as with procedures under § 2703(d), the second prong of the First Amendment analysis is most important. Doc. 45 at 25-26. They contend that Magistrate Judge Buchanan erroneously ignored the positive role that openness in § 2703 proceedings would serve, and thus misapplied the *Goetz* standard to this case.

In *Goetz*, the Fourth Circuit rejected the claim that search warrant affidavits must be open to public inspection under the First Amendment because it did not meet the "history" prong of the First Amendment analysis, noting that historically, proceedings for the issuance of search warrants were not open. *Goetz*, 886 F.2d at 64. Though disposing of the First Amendment claim on the first prong, the Fourth Circuit went on to provide guidance about the so-called "logic" prong. As the Fourth Circuit observed of search warrants, "the affidavit may describe continuing investigations, disclose information gleaned from wiretaps that have not yet been terminated, or reveal the identity of informers whose lives would be endangered." *Goetz*, 886 F.2d at 64. The Fourth Circuit also noted that the need for sealing affidavits may remain after execution or after indictment. As the court said, "[f]requently—probably most frequently—the warrant papers including supporting affidavits are open for inspection by the press and public in the clerk's office after the warrant has been executed. But this is not demanded by the first amendment." *Goetz*, 886 F.2d at 64.

The Court holds that the concerns articulated in *Goetz* are dispositive here. The procedures for obtaining a § 2703 order are modeled after search warrant procedures, such as those at issue in *Goetz*, and the same concerns about secrecy apply to the applications, affidavits, and other records sought. The application submitted for the § 2703 order contains sensitive information, and provides the judicial officer reviewing the government's application with crucial context and background information about the investigation. Based on a thorough review

of the affidavits, the Court concludes that the application for the Twitter Order contains extremely sensitive information, and disclosure at this point would have a significant likelihood of jeopardizing the government's investigation. Moreover, Petitioners seek an extraordinary remedy, the pre-execution disclosure of supporting affidavits, whereas in *Goetz*, the claimants sought only post-execution disclosure. *Goetz*, 886 F.2d at 62. Petitioners question whether disclosure of secret affidavits would lead to destruction or removal of evidence in this case since § 2703 orders are directed at third parties, not the subjects of the investigation. Doc. 45 at 27. As noted above, however, electronic evidence may be more prone to destruction or removal than physical evidence. Even if Twitter has already preserved information sought by the Twitter Order, others may be able to destroy other sensitive information not under Twitter's control.

Petitioners also claim that routine disclosure of § 2703 activities would improve the functioning of the judicial system, but this argument is unpersuasive. As the Supreme Court observed in *Press-Enterprise II*: "Although many governmental processes operate best under public scrutiny, it takes little imagination to recognize that there are some kinds of government operations that would be totally frustrated if conducted openly." 478 U.S. at 8-9. As with search warrant proceedings, judicial review provides pre-issuance screening of applications under § 2703(d). The Court can see no marked improvement that would result from recognition of a new First Amendment right of access to § 2703 application affidavits. The Court therefore concludes that Petitioners have no First Amendment right of access to the application for the Twitter Order or any other § 2703 orders sought in this investigation.

Finally, Petitioners request public docketing of all other § 2703 orders related to this investigation, including identification of each document and the date of filing. They request information sufficient to inform the public "whether an entry on the EC list refers to a § 2703

order, a pen register order, a trap and trace order, or some other type of order" entered in the course of an investigation, as well as allowing notice of whether the Court has denied such requests. Doc. 64 at 16. They insist that the law requires "individual docket entries for each event" entered into the court's files, such as documents or hearings. Doc. 64 at 16-17, 19.

The Court has examined the Clerk's docketing procedures thoroughly and finds them constitutionally acceptable. The public running list includes information showing that a particular docket is a criminal case, the date of assignment, the presiding judge, the fact that it is under seal, and other information. The running list does not provide more detailed docketing of each matter, such as the date when a particular § 2703 order, warrant, subpoena, or other order was docketed. Such detailed docketing would allow Petitioners (and many others) to observe the progress of a particular investigation, or to analyze the correspondence between government activity and docketing of sealed orders, or even the investigative methodology in a particular case, permitting inferences about the contents of sealed records. Petitioners have no First Amendment right to this information for the reasons stated above.[25] Neither history nor logic supports Petitioners' claim that the First Amendment guarantees docketing of all information sought by Petitioners, and the Court holds that Petitioners' First Amendment claim fails.

2. Common Law

Magistrate Judge Buchanan also held that the common law right of access to the sealed records is outweighed by the government's interest in continued sealing, despite the public's interest in debating privacy issues and Wikileaks. Doc. 38 at 18-19; *see Nixon v. Warner*

[25] Moreover, the Clerk's procedures fall well within the standards adopted by the Judicial Conference on March 17, 2009, which allowed individual courts discretion to include information in excess of the case name and number. The fact that the Southern District of Texas has chosen a more public course presents no contrary argument. The Clerk has appropriately and adequately provided public notice of the judicial records sought by Petitioners, and Magistrate Judge Buchanan appropriately denied Petitioners' request for additional information.

Communications, Inc., 435 U.S. 589, 597-98 (1978); *Media General*, 417 F.3d at 429; *Virginia Dep't of State Police*, *supra*, 386 F.3d at 574. She found that the sealing order here involves a variety of interests sufficient to justify secrecy under the common law right of access, namely, the integrity of the investigation, the safety of law enforcement officers, preventing destruction of evidence, protecting witnesses from retaliation or intimidation, and preventing unnecessary exposure of those who may be under investigation but are later exonerated. Doc. 38 at 18; *see also Douglas Oil Co.*, *supra*, 441 U.S. at 219; *Media General*, 417 F.3d at 429; *Va. Dep't of State Police*, 386 F.3d at 575. She rejected Petitioners' contentions that the traditional reasons for secrecy are obviated because of publicity surrounding the Twitter Order, and that the government's interest in sealing no longer outweighs the public's interest. Doc. 38 at 19. As Magistrate Judge Buchanan reasoned:

> Petitioners' argument ignores the significant difference between revealing the existence of an investigation, and exposing critical aspects of its nature and scope. The sealed documents at issue set forth sensitive nonpublic facts, including the identity of targets and witnesses in an ongoing criminal investigation. Indeed, petitioners present no authority for the proposition that the public has a right of access to documents related to an ongoing investigation. *Cf. In the Matter of Application and Affidavit for a Search Warrant*, 923 F.2d 324, 326 (4th Cir. 1991)(affirming decision to unseal affidavit only after investigation had concluded).

Doc. 38 at 19. The Court sees no reason to disturb Magistrate Judge Buchanan's findings. To the contrary, accepting Petitioners' position would create perverse incentives. For example, a party could leak a controversial sealed document to the press, then point to the ensuing publicity as evidence that further sealing is unnecessary. The Court declines to set that precedent.

Petitioners also argue that Magistrate Judge Buchanan "erroneously concluded that the common law presumption of access to judicial records 'may be overcome by a countervailing government interest.'" Doc. 45 at 25. They contend that the government's countervailing

interests must "heavily outweigh" the public interests in access, and that Magistrate Judge Buchanan violated the "strict procedural requirements" set forth in *Media General*. Docs. 45 at 25; 56 at 24. The government responds that Magistrate Judge Buchanan correctly stated the standard, and that the language cited by Petitioners is immaterial to the actual standard applied, and that even if it is not, Petitioners failed to show that a different standard would cause a different result. Doc. 45 at 25.

Magistrate Judge Buchanan clearly cited and applied the standards set forth by the Fourth Circuit in *Media General*. The Fourth Circuit there held that the government's interest in continuing its ongoing criminal investigation outweighed the petitioners' interest in having only one document opened to the press and public. 417 F.3d at 430-31. Petitioners argue that *Rushford v. New Yorker Magazine*, 846 F.2d 249, 253 (4th Cir. 1988) holds that the common law presumption of openness falls only to a countervailing government interest that "heavily outweighs" the public interest in disclosure. In *Media General*, by contrast, the Fourth Circuit relied heavily on *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 66 (4th Cir. 1989) and *In re Knight Pub. Co.*, 743 F.2d 231, 235 (4th Cir. 1984), neither of which referred to a "heavily outweigh" standard. In any event, *Media General*, *Goetz*, and *Rushford* all relied on the standard supplied by the United States Supreme Court in *Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978). The Court therefore declines to read an inconsistency into the Fourth Circuit's use of "outweigh" in *Media General* and *In re Knight Pub.*, and its use of "heavily outweigh" in *Rushford*. If there is a material distinction between the standards set forth in those cases (and the Court does not believe that there is) it is too slender to support Petitioners' objection.

Moreover, Magistrate Judge Buchanan provided the explanation of her sealing decisions required by *Media General*. "Where, as here, the government's explanations and the judicial

officer's reasons for sealing are patently apparent upon consideration of the documents at issue and when the record provides sufficient information for appellate review, there is no requirement that the district court or magistrate judge prepare separate, detailed orders." *Media General*, 417 F.3d at 431. There is no need, as Petitioners put it in one pleading, "to proceed document-by-document[.]" Doc. 58 at 34-35. The balancing that the magistrate judge performed here considers the effects that disclosure would have upon the public debate and the harms to the government's investigation that could—and probably would—result from unsealing.

The United States clearly has a compelling interest in protecting its ongoing investigation here, and Magistrate Judge Buchanan appropriately denied Petitioners' common law request for unsealing the application and supporting materials. *See ACLU v. Holder*, --- F.3d ---, 2011 WL 1108252, at *7 (4th Cir. 2011) ("The United States has a compelling interest in protecting the integrity of ongoing fraud investigations.") (citing *Virginia Dep't of State Police*, 386 F.3d at 579). For the same reason, Magistrate Judge Buchanan properly rejected Petitioners' argument that their own interest or the public interest outweighs the government's interest in secrecy.

Petitioners also challenge Magistrate Judge Buchanan's refusal to order unsealing and public docketing of all orders in this investigation that may be addressed to service providers other than Twitter. For the reasons outlined above, the government's interest in secrecy outweighs the interests favoring disclosure. As noted before, a docket sheet for § 2703 orders containing the information requested would disclose the progress of the government investigation in significant detail. The Court has reviewed the Clerk's current docketing procedures and holds that they adequately satisfy common law sealing criteria.

The Court does not hold that the records at issue may be sealed indefinitely. The Court holds only that Petitioners' motions must be denied without prejudice, and that the particular

records sought should remain under seal for now.

III. CONCLUSION

For the foregoing reasons, Petitioners' objections to Magistrate Judge Buchanan's orders will be DENIED. The Clerk is directed to forward copies of this Memorandum Opinion to all counsel of record.

November 10, 2011
Alexandria, Virginia

/s/
Liam O'Grady
United States District Judge